REMARKS

Applicant respectfully requests consideration of the subject application as amended herein. This Amendment is submitted in response to the Office Action mailed on July 26, 2007. Claims 1-24 are rejected. In this Amendment, claims 1-3, 13-15, 18 and 20 have been amended. No new matter has been added. No claims have been canceled. Therefore, claims 1-24 are presented for examination.

Summary of Rejections

Claims 1-4, 6-16 and 18-24 stand rejected under 35 U.S.C. 102(e) as being anticipated by Gehrmann et al. (U.S. Pub. No. 2004/0176071, hereinafter "Gehrmann").

Claims 5 and 17 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Gehrmann.

Claims 1, 2 and 13 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1, 2, 11, 15, 19 and 23 of co-pending Application No. 10/977,158 (U.S. Publication No. 2006/0075259).

Claim Rejections under 35 U.S.C. § 112

Claims 3 and 9 stand rejected under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 1 has been amended such that claims 3 and 9 are placed in a definite form. Therefore, applicant respectfully requests that Examiner remove his rejections under 35 U.S.C. § 112.

Claims 1-12

Claims 1-4, 6-16 and 18-24 stand rejected under 35 U.S.C. 102(e) as being anticipated by Gehrmann. Claims 5 and 17 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Gehrmann.

As amended, claim 1 recites:

> A method comprising:
> exchanging **unencrypted data** between a SIM device and an application executed in a trusted platform via a trusted path within a computer system, the trusted path being a path through a trusted port of a chipset, wherein the **trusted port is mapped to a protected section of memory that is inaccessible to direct memory access**, wherein the unencrypted data to be exchanged is secured from unauthorized access.

(emphasis added).

Gehrmann discloses securing data transmitted between a subscription module and a device into which the subscription module is inserted, or between a subscription module and a remote device, **by encrypting the data**. (Gehrmann, paragraph [0060]; paragraph [0057], lines 17-24; paragraph [0022]). For example, Gehrmann states that, "preferably, in order to protect the communication between the RAA client and the subscription module, all messages sent between the entities are encrypted with a symmetric encryption algorithm." (Gehrmann, paragraph [0066], lines 8-11). Gehrmann further states, for example, "after successful authentication and key exchange, the actual data exchange between the client communications terminal and the subscription module may be initiated in step 506, preferably using a symmetric encryption algorithm." (Gehrmann, paragraph [0085], lines 1-5). In contrast, claim 1 recites, "**exchanging unencrypted data** ... wherein the unencrypted data is secured from unauthorized access." Gehrmann fails to disclose exchanging unencrypted data that is secured from unauthorized access.

The current Office Action states:

> [T]he client communications terminal corresponds to applicant's "an application executed in a trusted platform, via a trusted path within a computer system (e.g., par. [0065] and [0084]), the trusted path being a path through a trusted port" ("... The subscription module further comprises a input/output interface 206 for communication with the device it is inserted in..." – e.g., par. [0060], "... the communication over the interface provided by the subscription module, is protected" – 1.g., par. [0022], "... a wireless interface and the subscription module may be implemented as one physically inseparable entity" – e.g., par. [0032], "... Therefore, it is an advantage of the invention that it secures all interfaces when providing remote access..." – e.g., par. [0061], [0037] and Fig. 2). Please note protected interface and secures all interfaces correspond to applicant's trusted port of a chipset (e.g., par. [0036], [0038], [0040], [0049] and [0064]-[0065]). Please note subscription module, processing means, circuit and communication means correspond to applicant's chipset, wherein the data to be exchanged is secured from unauthorized access, "thereby providing a considerably improved security against unauthorized use of the sensitive information on the subscription module," e.g., paragraph [0013], "After successful authentication and key exchange, the actual data exchange between the client communications terminal and the subscription module may be initiated in step 506, preferably using a symmetric encryption algorithm, as described in connection with Fig. 5...." – e.g., paragraph [0085] and "Furthermore, in order to further protect the communication between the RAA client and the subscription module, all messages sent between the entities are integrity protected, as described in connection with Fig. 5 ..." – e.g., paragraph [0086].

(Office Action, 7/26/2007, pages 4-5).

Applicants respectfully disagree with Examiner's assertion that Gehrmann discloses an application executed in a trusted platform, via a trusted path within a computer system. Gehrmann discloses securing data transmissions through authentication and encryption. (see, for example, Gehrmann, paragraph [0060]; paragraph [0057], lines 17-24; paragraph [0022]; paragraph [0066], lines 8-11; paragraph [0085], lines 1-5). Nowhere does Gehrmann disclose using a trusted platform or a trusted path to secure data. Therefore, in order to secure any path disclosed in Gehrmann, authentication and encryption must be used. Moreover, if the platform of Gehrmann was a trusted platform that included a trusted path, then no encryption or authentication would be necessary to secure the data transmitted over

the path.

Nevertheless, applicants have amended claim 1 to further clarify that a trusted port is mapped to a protected section of memory that is inaccessible to direct memory access. Gehrmann does not disclose a protected section of memory that is inaccessible to direct memory access, much less a trusted port that is mapped to such a protected section of memory.

For the above reasons, claim 1 and its dependent claims are patentable over Gehrmann. Accordingly, applicants respectfully request that Examiner remove his rejections to claim 1 and its dependent claims under 35 U.S.C. 102(e) and 35 U.S.C. 103(a).

Claims 13-24

Claims 1-4, 6-16 and 18-24 stand rejected under 35 U.S.C. 102(e) as being anticipated by Gehrmann. Claims 5 and 17 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Gehrmann.

As amended, claim 13 recites:

> A system comprising:
> a processor;
> a memory having a protected section that is **inaccessible to direct memory access** and an unprotected section that is accessible to direct memory access;
> a SIM device; and
> a chipset having **a trusted port mapped to the protected section of the memory to exchange unencrypted data** between the SIM device and an application executed in a trusted platform, wherein the unencrypted data to be exchanged is secured from unauthorized access.

(emphasis added).

Gehrmann discloses securing data transmitted between a subscription module and a device into which the subscription module is inserted, or between a subscription module and a remote device, **by encrypting the data**. (Gehrmann, paragraph [0060]; paragraph [0057],

lines 17-24; paragraph [0022]). For example, Gehrmann states that, "preferably, in order to protect the communication between the RAA client and the subscription module, all messages sent between the entities are encrypted with a symmetric encryption algorithm." (Gehrmann, paragraph [0066], lines 8-11). Gehrmann further states, for example, "after successful authentication and key exchange, the actual data exchange between the client communications terminal and the subscription module may be initiated in step 506, preferably using a symmetric encryption algorithm." (Gehrmann, paragraph [0085], lines 1-5). In contrast, claim 13 recites, "**a trusted port mapped to the protected section of the memory to exchange unencrypted data** ... wherein the unencrypted data to be exchanged is secured from unauthorized access." Gehrmann fails to disclose exchanging unencrypted data that is secured from unauthorized access.

The current Office Action states:

> [T]he client communications terminal corresponds to applicant's "an application executed in a trusted platform, via a trusted path within a computer system (e.g., par. [0065] and [0084]), the trusted path being a path through a trusted port" ("... The subscription module further comprises a input/output interface 206 for communication with the device it is inserted in..." – e.g., par. [0060], "... the communication over the interface provided by the subscription module, is protected" – 1.g., par. [0022], "... a wireless interface and the subscription module may be implemented as one physically inseparable entity" – e.g., par. [0032], "... Therefore, it is an advantage of the invention that it secures all interfaces when providing remote access..." – e.g., par. [0061], [0037] and Fig. 2). Please note protected interface and secures all interfaces correspond to applicant's trusted port of a chipset (e.g., par. [0036], [0038], [0040], [0049] and [0064]-[0065]). Please note subscription module, processing means, circuit and communication means correspond to applicant's chipset, wherein the data to be exchanged is secured from unauthorized access, "thereby providing a considerably improved security against unauthorized use of the sensitive information on the subscription module," e.g., paragraph [0013], "After successful authentication and key exchange, the actual data exchange between the client communications terminal and the subscription module may be initiated in step 506, preferably using a symmetric encryption algorithm, as described in connection with Fig. 5...." – e.g., paragraph [0085] and "Furthermore, in order to further protect the communication between the RAA client and the subscription module, all messages sent between the entities are integrity protected, as described in

connection with Fig. 5 ..." – e.g., paragraph [0086].

(Office Action, 7/26/2007, pages 4-5).

Applicants respectfully disagree with Examiner's assertion that Gehrmann discloses an application executed in a trusted platform, via a trusted path within a computer system. Gehrmann discloses securing data transmissions through authentication and encryption. (see, for example, Gehrmann, paragraph [0060]; paragraph [0057], lines 17-24; paragraph [0022]; paragraph [0066], lines 8-11; paragraph [0085], lines 1-5). Nowhere does Gehrmann disclose using a trusted platform or a trusted path to secure data. Therefore, in order to secure any path disclosed in Gehrmann, authentication and encryption must be used. Moreover, if the platform of Gehrmann was a trusted platform that included a trusted path, then no encryption or authentication would be necessary to secure the data transmitted over the path.

Nevertheless, applicants have amended claim 13 to further clarify that a trusted port is mapped to a protected section of memory that is inaccessible to direct memory access. Gehrmann does not disclose a protected section of memory that is inaccessible to direct memory access, much less a trusted port that is mapped to such a protected section of memory.

For the above reasons, claim 13 and its dependent claims are patentable over Gehrmann. Accordingly, applicants respectfully request that Examiner remove his rejections to claim 13 and its dependent claims under 35 U.S.C. § 102(e) and 35 U.S.C. § 103(a).

Double Patenting

Claims 1, 2 and 13 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1, 2, 11, 15, 19 and 23 of co-pending Application No. 10/977,158 (U.S. Publication No. 2006/0075259).

Claims 1-2

The applicants respectfully submit that claims 1 and 2 of the present application are patently distinct from the referenced claims of co-pending Application No. 10/977,158. As amended, claim 1 recites:

> A method comprising:
> exchanging unencrypted data between a SIM device and an application executed in a trusted platform via a trusted path within a computer system, the trusted path being a path through a trusted port of a chipset, **wherein the trusted port is mapped to a protected section of memory that is inaccessible to direct memory access**, wherein the unencrypted data to be exchanged is secured from unauthorized access.

(emphasis added).

None of the referenced claims of co-pending Application No. 10/977,158 claim a protected section of memory that is inaccessible to direct memory access. In contrast, claim 1 discloses a trusted port that is mapped to a protected section of memory that is inaccessible to direct memory access. Moreover, claims 1, 2, 11, 15, 19 and 23 of co-pending Application No. 10/977,158 include the limitation, "to generate a session key to encrypt data to be transmitted between the device and the application." Neither claim 1 nor claim 2 include such a limitation. Accordingly, applicants respectfully assert that the claims 1 and 2 are patently distinct from claims 1, 2, 11, 15, 19 and 23 of co-pending Application No. 10/977,158, and respectfully request that Examiner remove his rejections to claims 1 and 2 for double patenting.

Claim 13

The applicants respectfully submit that claim 13 of the present application is patently distinct from the referenced claims of co-pending Application No. 10/977,158. As amended, claim 13 recites:

> A system comprising:
> a processor;
> a memory having a protected section that is **inaccessible to direct memory access** and an unprotected section that is accessible to direct memory access;
> a SIM device; and
> a chipset having **a trusted port mapped to the protected section of the memory to exchange unencrypted data** between the SIM device and an application executed in a trusted platform, wherein the unencrypted data to be exchanged is secured from unauthorized access.

(emphasis added).

None of the referenced claims of co-pending Application No. 10/977,158 claim a protected section of memory that is inaccessible to direct memory access. In contrast, claim 13 discloses a trusted port that is mapped to a protected section of memory that is inaccessible to direct memory access. Moreover, claims 1, 2, 11, 15, 19 and 23 of co-pending Application No. 10/977,158 include the limitation, "to generate a session key to encrypt data to be transmitted between the device and the application." Claim 13 does not include such a limitation. Accordingly, applicants respectfully assert that claim 13 is patently distinct from claims 1, 2, 11, 15, 19 and 23 of co-pending Application No. 10/977,158, and respectfully request that Examiner remove his rejections to claim 13 for double patenting.

Conclusion

Accordingly, Applicant respectfully requests the withdrawal of the rejections and submits that pending claims 1-24 are in condition for allowance. Applicant respectfully requests reconsideration of the application and allowance of the pending claims.

If the Examiner determines the prompt allowance of these claims could be facilitated by a telephone conference, the Examiner is invited to contact Benjamin Kimes at (408) 720-8300.

Deposit Account Authorization

Authorization is hereby given to charge our Deposit Account No. 02-2666 for any charges that may be due. Furthermore, if an extension is required, then Applicant hereby requests such extension.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR
& ZAFMAN LLP

Dated: 10/24/07

By _____
Benjamin A. Kimes
Reg. No. 50,870

1279 Oakmead Parkway
Sunnyvale, CA 94085-4040
(408) 720-8300

Customer No. 008791